CLAIMS

What is claimed is:

1. A method for use in analyzing network security, comprising:

constructing query-based rules to be used to identify network conditions.

2. The method of claim 1, wherein network conditions include vulnerability conditions and intrusion conditions.

3. The method of claim 1, wherein the step of constructing query-based rules includes constructing query-based rules from a set of lexical elements that includes a set of templates.

4. The method of claim 3, wherein the templates are divided into two classes comprising template types and template actions.

5. The method of claim 1, wherein the step of constructing query-based rules includes constructing query-based rules from a set of lexical elements that includes a set of statements, a set of templates, and a set of reserved words.

6. The method of claim 5, wherein:

network conditions include vulnerability conditions and intrusion conditions;

the set of statements includes SET and SELECT;

the set of reserved words includes AND, TO, and WHERE; and

the set of templates includes:

for identifying network vulnerability conditions:

Operating System, Host, Protocol, Application, Vulnerability, Port, Execute, ExecuteHex, Contains, and ContainsHex;

for identifying network intrusion conditions:

Operating System, Protocol, Application, Port, Length, Offset, Threshold, Contains, ContainsHex, Flags, FragmentID, IcmpType, IcmpCode, PayloadSize, and TimeToLive.

7. The method of claim 1, wherein the step of constructing query-based rules includes associating each rule with an operating system.

8. A method for use in analyzing network security, comprising:

constructing rules to be used to identify network conditions, including vulnerability conditions and intrusion conditions, from a set of lexical elements that include a set of templates, where each rule for identifying a vulnerability condition is associated with an operating system.

9. The method of claim 8, wherein the set of lexical elements further includes a set of statements and a set of reserved words.

10. The method of claim 8, wherein the templates in the set of templates are classified in one of two classes comprising template types and template actions.

11. A method for use in analyzing network security, comprising:

constructing a set of rules to be used to identify vulnerability conditions and intrusion conditions from a set of lexical elements that include a set of templates, where each rule for identifying a vulnerability condition is associated with an operating system; and

wherein the set of templates includes:

for identifying network vulnerability conditions:

Host, Protocol, Application, Vulnerability, Port, Execute, ExecuteHex, Contains, and ContainsHex;

for identifying network intrusion conditions:

Protocol, Application, Port, Length, Offset, Threshold, Contains, ContainsHex, Flags, FragmentID, IcmpType, IcmpCode, PayloadSize, and TimeToLive.

12. The method of claim 11, wherein the set of lexical elements further includes:

a set of reserved words, including AND, TO, and WHERE;

a set of statements, including SET and SELECT.

13. A vulnerability detection system comprising:

a rule constructor that allows a user to construct rules based on specified lexical elements, where the rules are to be used to identify vulnerability conditions in a network.

14. The vulnerability detection system of claim 13, wherein the lexical elements include a set of statements, a set of templates, and a set of reserved words.

15. The vulnerability detection system of claim 13, wherein:

the rule constructor includes a graphical user interface to receive information from a user constructing a rule; and

the rule, once constructed, is stored in a rule database.

16. The vulnerability detection system of claim 13, wherein the rule constructor requires each rule to be associated with an operating system.

17. A system for use in network security, comprising:

a rule constructor that allows a user to construct rules based on specified lexical elements, where the rules are to be used to identify vulnerability conditions in a network;

a database for storing the rules; and

a vulnerability detector designed to gather information about a network and to use that information along with the stored rules to determine if a vulnerability condition exists on the network.

18. A vulnerability detection system, comprising:

a rule database that includes rules that are based on specified lexical elements, including a set of templates, wherein the rules are to be used to identify vulnerability conditions on a network.

19. The vulnerability detection system of claim 18, wherein the lexical elements further include a set of statements and a set of reserved words.

20. The vulnerability detection system of claim 18, wherein each rule is associated with a specified operating system.

21. An intrusion detection system comprising:

a rule constructor that allows a user to construct rules based on specified lexical elements, where the rules are to be used to identify intrusion conditions in a network.

22. The intrusion detection system of claim 21, wherein

the lexical elements include a set of statements, a set of templates, and a set of reserved words.

23. The intrusion detection system of claim 21, wherein:

the rule constructor includes a graphical user interface to receive information from a user constructing a rule; and

the rule, once constructed, is stored in a rule database.

24. A system for use in network security, comprising:

a rule constructor that allows a user to construct rules based on specified lexical elements, where the rules are to be used to identify intrusion conditions in a network;

a database for storing the rules; and

an intrusion detector designed to monitor network traffic and to check that network traffic against the stored rules to determine if an intrusion condition exists on the network, the intrusion detector further designed to notify a user of the presence of an intrusion condition, but only if the intrusion condition is applicable to the network.

25. An intrusion detection system, comprising:

a rule database that includes rules that are based on specified lexical elements, including a set of templates, wherein the rules are to be used to identify intrusion conditions on a network.

26. The intrusion detection system of claim 25, wherein the lexical elements further include a set of statements and a set of reserved words.

27. A computer readable medium on which is stored a set of instructions, which when executed, cause the performance of the following steps:

storing a set of rules to be used to identify vulnerability conditions and intrusion conditions, which rules are constructed from a set of lexical elements that include a set of templates, where each rule to identify a vulnerability condition is associated with an operating system.

28. The method of claim 27, wherein the set of lexical elements further includes a set of statements and a set of reserved words.

29. The method of claim 27, wherein the templates in the set of templates are classified in one of two classes comprising template types and template actions.